HackRF实现GPS欺骗教程

GPS (/blog/tag/metorm/GPS) HackRF (/blog/tag/metorm/HackRF) 2019-05-28 10:38:32
0 0 0

硬件平台：HackRF One
软件平台：MAC运行环境搭建
系统平台：OS X 10.11 El Capitan
GPS终端：One Plus手机，飞行模式，仅GPS定位，GPS test App
文章特点：根据网上的文章实验证明发现了问题总结归纳到此，针对以上环境担保100%成功。

---

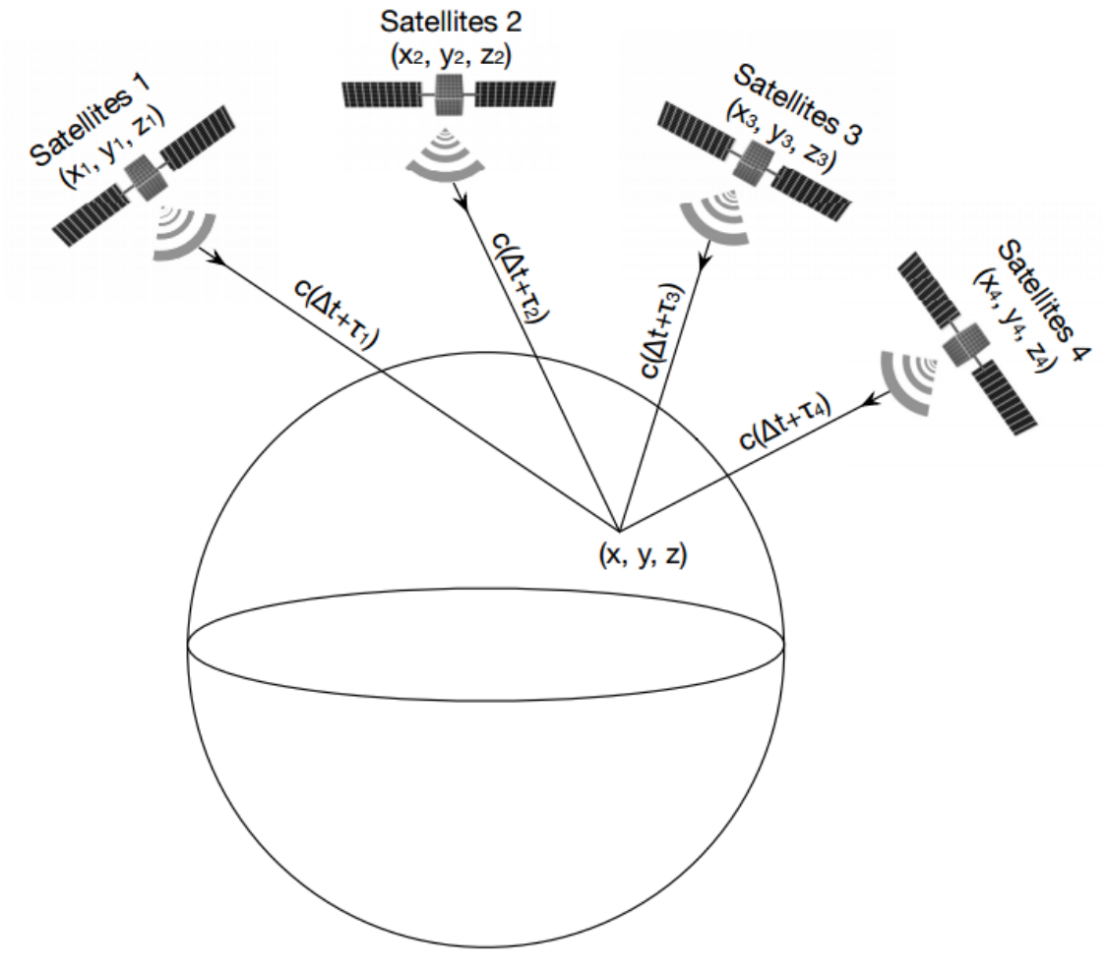
0. GPS系统简介

GPS 系统本身非常复杂, 涉及到卫星通信等各个领域. 这里只是简单介绍一下. 我们通常所说的 GPS 全球定位系统是由美国国防部建造完成. 目前在太空中共有31颗卫星在同时运作. 一般我们需要至少4颗卫星来完成三角定位. GPS卫星同时发送民用L1和军用L2两种无线信号. 我们通常使用的是没有加密的L1民用 1575.42MHz 的超高频波段.

GPS 信号里包含了3种常用信息.

1. Pseudorandom code: 简单的ID 码, 用来识别每颗卫星.
2. Ephemeris data: 包含卫星的运行状态, 时间日期等信息. 这在通过卫星来定位起到非常重要的作用.
3. Almanac data: 包含有每颗卫星的轨道信息, 以及卫星在某个特定时段将出现的具体位置.

内容摘自王康的PDF，下载地址见附录：



(htt

p://images2015.cnblogs.com/blog/640760/201601/640760-20160127175136457-231534131.png)

1) GPS定位原理

首先，让我们明确我们的需求。我们想要知道的是我们的位置坐标(x,y,z)，如果从一个已知坐标(x1,y1,z1)的点A（这个点在现实情况下是卫星）广播一个信号，比如说光和声音或者电磁波，然后我们试着去测量信号发送至到达的时间差τ1（在gps系统中我们用的是电磁波，我们知道它的速度），然后我们就能得出下面的等式：

$$\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}=c\tau_1$$ (htt

p://images2015.cnblogs.com/blog/640760/201601/640760-20160127175204395-1924484312.png)

这个等式有3个未知变量，因此单单一个等式解不出来，我们可以再加两个已知位置的点（卫星），我们把它们记作(x2,y2,z2) 和 (x3,y3,z3)，然后就是下面的方程组

$$\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}=c\tau_1$$
$$\sqrt{(x-x_2)^2+(y-y_2)^2+(z-z_2)^2}=c\tau_2$$
$$\sqrt{(x-x_3)^2+(y-y_3)^2+(z-z_3)^2}=c\tau_3$$

(http://images2015.cnblogs.com/blog/640760/201601/640760-20160127175228723-794473054.png)

现在我们就能解出我们的位置(x,y,z)了

但在工程应用中这样还不够。为了测量电磁波发送至到达的时间差τ1，需要在电磁波发送的时候写一个时间戳t1，然后是卫星上的时钟时间参考值，当信号到达我们这里时，我们提取出时间戳t1，然后计算t1和当地时间t2的差值来计算时间差τ1。然而当地时间和卫星时间并不是同步的，会出现一个时间偏移量Δt1，所以这个时间偏移量也要被考虑进去，于是修正后的方程式如下所示：

$$\sqrt{(x-x_i)^2+(y-y_i)^2+(z-z_i)^2}=c(\Delta t_i+\tau_i), i\in\{1,2,3\}$$

(http://images2015.cnblogs.com/blog/640760/201601/640760-20160127175309895-1612779133.png)

译者注：所以有4个变量，就需要4个卫星来创造4个等式啦，以下高等数学内容略，以上内容说明我们需要伪造至少4颗卫星的信号才能使gps定位

TABLE I
GPS L1 SIGNAL

Parameter	Value
Code	C/A Code
Modulation	BPSK
Frequency	1575.42MHz
Code Rate	1.023 MHz

(http://images2015.cnblogs.com/blog/640760/201601/640760-20160127175338832-942045540.png)

1. 下载编译gps-sdr-sim

因为我的OSX系统下使用MacPorts安装了gcc5，xcode默认安装的gcc是/usr/bin/gcc，所以直接make可能会提示找不到omp.h文件因为调用的是xcode的gcc(苹果xcode安装的gcc很多程序都无法成功编译)，那么按照下面的步骤即可正常安装。

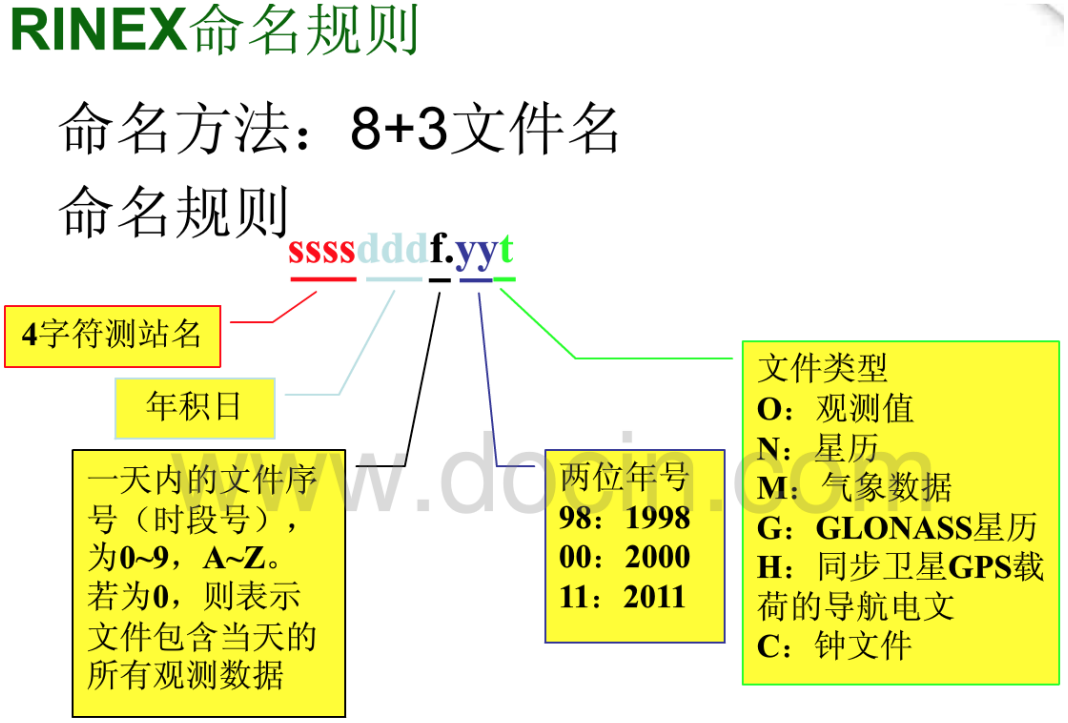
```
1. $ git clone https://github.com/osqzss/gps-sdr-sim.git
2. $ cd gps-sdr-sim
3. $ gcc-mp-5 gpssim.c -lm -O3 -o gps-sdr-sim
```

或者干脆sudo port select gcc mp-5再make就OK了

2. RINEX星历数据下载

```
1. ftp://cddis.gsfc.nasa.gov/pub/gps/data/daily/2016/brdc
```

找brdc0050.16n.Z 这样的文件，解压出来就是了



(http://images2015.cnblogs.com/blog/640760/201601/640760-20160127175543082-2139318812.png)

3. 生成GPS仿真数据

```
1. $./gps-sdr-sim -e brdc3540.14n -l 29.643598,91.101319,100 -b 8
```

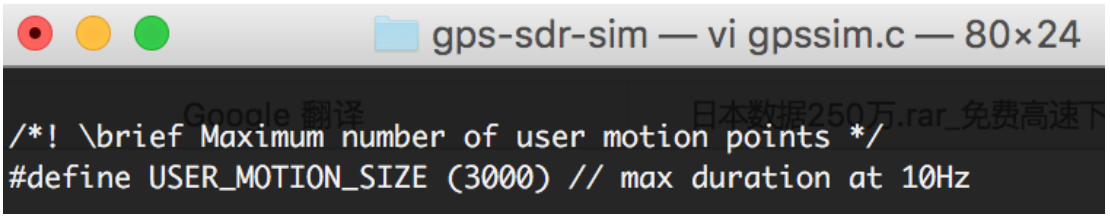
指定星历文件(可自行更新至最新的星历数据)，设置经纬度(拉萨市)，**必须指定采样精度为8**否则用hackRF one欺骗成功率不高,反正我指定16是没成功过(默认为16，乌云文章也是16但设备是bladeRF)

另外如果有其他目的也可以伪造一个动态的GPS数据样本，例如欺骗计步器，轨迹等

```
1. $./gps-sdr-sim -e brdc3540.14n -u circle.csv -b 8
```

GPS-SDR-SIM 运行时间问题

默认情况下GPS模拟器只能连续工作5分钟左右. 通过查看源代码后, 我们可以发现这是因为程序默认设置导致. 在程序设计之初为了节省硬盘空间, 默认只生成了300秒左右的数据. 我们可以通过改动参数来延長工作時間. 但需要注意的是仅仅延長到15分鐘，數據便可達到5G大小.



(http://images2015.cnblogs.com/blog/640760/201601/640760-20160127175659098-2061437423.png)

4. HackRF发射GPS数据

```
1. $ hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
   -R
```

指定GPS数据，指定频率为1575420000 即民用GPS L1波段频率，指定采样速率2.6Msps，开启天线增益，指定TX VGA(IF)为0(为了限制影响范围，最大为47慎用！！！)，最后开启重复发射数据功能

手机终端1分40秒就可以被欺骗成功，这里有一个测试技巧，就是定模模式选仅GPS定位，不要用基站、WLAN定位，这样打开地图等软件就是伪造后的GPS坐标点。

Pre: Hack RF 入手和入门 (/blog/post/metorm/%E5%85%A5%E6%89%8B%E5%92%8C%E5%85%A5%E9%97%A8)

Next: V2EX 提供的 Android Captive Portal Server 地址 (/blog/post/metorm/V2EX-%E6%8F%90%E4%BE%9B%E7%9A%84-Android-Captive-Portal-Server-%E5%9C%B0%E5%9D%80)

(/blog/metorm)

船长的日志 (/blog/metorm)

非典型导弹设计师

分类

导航

主页 (/blog/metorm)
关于 (/blog/single/metorm/About-Me)
归档 (/blog/archives/metorm)
标签 (/blog/tags/metorm)

友情链接

search